

Remarks

Claims 1 and 4-11 are pending in the application. Claims 1 and 4-11 are rejected. Claims 2-3 and 12-72 were cancelled previously. No new matter is added. The Claims are presented above for ease of references. The claims are not amended herein. All rejections are respectfully traversed.

The invention re-authenticates and protects wireless communication security. Using a key lease generated by performance of a primary authentication protocol, a secondary authentication protocol is performed between a wireless client electronic system (client) and a wireless network access point electronic system (AP). The key lease includes a key lease period for indicating a length of time in which the key lease is valid for using the secondary authentication protocol instead of the primary authentication protocol. If the secondary authentication protocol is successful, a session encryption key is generated for encrypting communication traffic between said client and said AP.

A hash function and encryption key from the key lease are applied to at least first and second random numbers to generate at least one session encryption key for use upon the successful completion of the secondary protocol. The invention is a useful solution to ensure the AP accepts replayed data frames upon subsequent performances of the secondary authentication protocol by wireless clients.

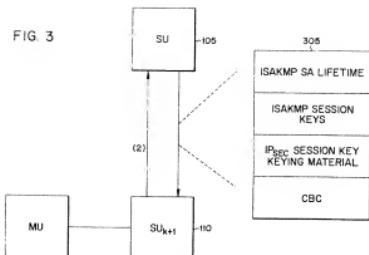
Claims 1 and 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng, et al., (U.S. 6,418,130 – “Cheng”) in view of Dole (U.S. 6,628,786).

Cheng describes a method for performing a hand off of a wireless mobile unit that re-uses existing security associations. Cheng explicitly teaches “reusing rather than renegotiating the security associations” corresponding to the mobile units once the mobile unit is handed over, see col. 2, lines 9-18. In contrast, claim 1 recites “performing a secondary authentication protocol between a wireless client electronic system (client) and a wireless network access point electronic system (AP) using a key lease generated by performance of a primary authentication protocol.” The invention performs a primary authentication protocol which generates a key lease that is used to perform the secondary authentication protocol. Cheng never performs a secondary authentication protocol, as claimed. Instead, Cheng reuses existing security associations for mobile unit hand-offs.

Further, the Examiner points to col. 6, lines 26-44, as teaching “performing a secondary authentication protocol,” as claimed. However, the Examiner will note that the referenced section at col. 6 describes, in conjunction with Figure 3, communications between so called stationary units (access points), rather than between a mobile client and an access point, as claimed.

Figure 3, below, shows two stationary units 105 and 110, exchanging security attributes:

FIG. 3



The section referenced by the Examiner details only communications between stationary units. In contrast, claimed is transmitting a key lease from the client to the AP, transmitting associated random numbers to both the client and AP, and if the secondary protocol is successful, generating a session encryption key for encrypting communication traffic between said client and said AP. In short, the performing step recites performing a secondary authentication protocol between a wireless client electronic system (client) and a wireless network access point electronic system (AP). The section cited by the Examiner describes communication, between stationary units, of data related to an already completed authentication, which data will be reused. Therefore, Cheng can never be used to make the invention obvious. The Examiner is respectfully requested to reconsider and withdraw the rejection based on Cheng.

Dole fails to cure the defect of Cheng. Dole describes a random number generation method used for encrypting communications between computers. The Examiner's assertion that Dole teaches generating a first random number associated with said client and a second random number associated with said AP as claimed, is pure conjecture because there is never any

description of associating random numbers with a computer such as a client or AP in col. 6, lines 5-27, see below:

5 Referring now to FIG. 3, a flowchart illustrating a method of implementing the present invention is presented. Normally, the method of the present invention will be implemented as a computer program ("application") residing on a host computer. However, it will be appreciated by
10 those skilled in the art that the method of the present invention may be implemented through the use of electronic hardware or through the use of a combination of hardware and software.

15 The random number generator is started with a request for random numbers (step 50). Normally, the internal state of the random number generator will have previously been set, based upon a prior operation. Next, the application will check to determine whether any additional sources of entropy have been received (step 52). Additional sources of
20 entropy may consist of prior secret session keys, nonces, private/public key pairs generated for encryption protocols such as RSA or random key values utilized to implement the Diffie-Hellman key exchange protocol. If no additional sources of entropy have been received, the application will proceed to generate random numbers based on the existing
25 internal state (step 60).

The Examiner is requested to specifically point out exactly which words above mean generating a first random number associated with said client and a second random number associated with said AP, as claimed. The applicants see only random number generation for encryption purposes. Further still, there is no teaching of a secondary authentication protocol, or re-authenticating.

The hashing described in Dole is for encryption of a particular message and has nothing to do with a secondary authentication protocol using a key lease from performance of a primary authentication protocol, as claimed.

Claims 7-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng in view of Dole, and in further view of Kessler, et al. (U.S. 6,789,147 – “Kessler”).

Claimed is using said encryption key, said first random number, said second random number, a first media access control (MAC) address associated with said client, a second media access control (MAC) address associated with said AP, and a hash function to determine said first and second session encryption keys. The section at col. 5, lines 18-27 referenced by the Examiner is silent as to generating first and second session encryption keys based on the explicitly recited elements above, see, e.g., col. 5, lines 29-32, below:

conjunction with FIGS. 3-8. Additionally, such security operations could include, but are not limited to, a request to (1) generate a random number, (2) generate a prime number, (3) perform modular exponentiation, (4) perform a hash operation, (5) generate keys for encryption/decryption, (6) perform a hash-message authentication code (H-MAC) operation, (7) perform a handshake hash operation and (8) perform a finish/verify operation.

There is nothing above that describes the explicitly claimed combination of elements to generate the first and second session keys, as claimed.

The same is true for the claimed applying a HMAC-MDS algorithm and said encryption key on a concatenation of said first random number, said second random number, said first media access control (MAC) address associated with said client, and said second media access control (MAC) address associated with said AP to determine said first session encryption key. There is no description of applying HMAC-MDS algorithm to the particular

concatenation to produce either a first or second session key as recited in the claims. The Examiner is also reminded that the invention re-authenticates using a second authentication protocol and a key lease from a primary authentication protocol. No such thing is ever taught by Cheng, Dole, or Kessler.

It is believed that this application is now in condition for allowance. A notice to this effect is respectfully requested. Should further questions arise concerning this application, the Examiner is invited to call Applicant's attorney at the number listed below.

Please charge any shortage in fees due in connection with the filing of this paper to Deposit Account 50-3650.

Respectfully submitted,
3Com Corporation,

By



Andrew J. Curtin
Attorney for the Assignee
Reg. No. 48,485

350 Campus Drive
Marlborough, MA 01752
Telephone: (508) 323-1330
Customer No. 56436